Journal of Pure and Applied Algebra 22 (1981) 121–129
North-Holland Publishing Company

GENERATORS OF $\mathrm{Sp}_n(V)$ OVER A QUASI SEMILOCAL SEMIHEREDITARY RING

Hiroyuki ISHIBASHI
Josai University, Saitama, Japan

Communicated by H. Bass
Received 18 June 1980

This paper is devoted to determine the minimal length of expressions of an isometry in a symplectic group $\mathrm{Sp}_n(V)$ by a product of transvections under the assumption that V is an n-ary nonsingular alternating space over a quasi semilocal semihereditary ring with 2 as a unit.

Introduction

Let $\circ$ be a quasi semilocal semihereditary ring, i.e., $\circ$ is a commutative ring with 1 which has finitely many maximal ideals $\{A_i \mid i \in I\}$ and the localization $\circ_{A_i}$ by any maximal ideal A_i is a valuation ring. We assume 2 is a unit in $\circ$. V is an n-ary free module over $\circ$ with a nonsingular symmetric alternating form. $\mathrm{Sp}_n(V)$ or $\mathrm{Sp}(V)$ is the symplectic group on V. An element σ of $\mathrm{Sp}(V)$ is called an isometry. If $\sigma \neq 1$ fixes a submodule of V which contains a hyperplane then we call it a transvection and the set of transvections is denoted by S.

For a submodule U of V, if there exist n vectors $x_1, \ldots, x_r, \ldots, x_n$ such that $U = \circ x_1 \oplus \cdots \oplus \circ x_r$ and $V = \circ x_1 \oplus \cdots \oplus \circ x_r \oplus \cdots \oplus \circ x_n$, then we call U a subspace of V and r the dimension of U; r is denoted by $\dim U$.

Let U be a subspace of V. We call U a line if $\dim U = 1$, a plane if $\dim U = 2$, and a hyperplane if $\dim U = n - 1$.

In the present paper we shall determine the minimal length $l(\sigma)$ of an expression of any isometry σ in $\mathrm{Sp}(V)$ by a product of elements in S. The result is

$$l(\sigma) = n - d \text{ or } n - d + 1,$$

where d is the rank of a maximal subspace of V which is contained in the fixed module of σ. In this paper, set-theoretic difference of A and B will be written $A - B$. $M \oplus N$ is a direct sum of modules M and N.

Clearly, this is a generalization of my paper [5].

1. Statement of the theorem

For i in I, let π_i or $^-$ be the canonical homomorphism from $\mathcal{O}$ onto $\bar{\mathcal{O}}=\mathcal{O}/A_i$. We use the same notation π_i or $^-$ to denote the canonical map from V onto $\bar{V}=V/A_iV$. We define canonically $\bar{x}+\bar{y}=\overline{x+y}$, $\bar{a}\bar{x}=\overline{ax}$ and $\bar{x}\bar{y}=\overline{xy}$ for x, y in V and a in $\mathcal{O}$. Since V is nonsingular, $\bar{V}$ is an n-ary nonsingular alternating space over the field $\bar{\mathcal{O}}$. For σ in $\mathrm{Sp}(V)$ we define $\bar{\sigma}$ in $\mathrm{Sp}(\bar{V})$ by $\bar{\sigma}\bar{x}=\overline{\sigma x}$, $x\in V$. Then the canonical map π_i or $^-$ from $\mathrm{Sp}(V)$ to $\mathrm{Sp}(\bar{V})$ defined by $\pi_i(\sigma)=\bar{\sigma}$ is a group homomorphism.

For a subset U of V, $U^*=\{x\in V\mid xU=0\}$. For submodules U and W of V, $U\perp W$ means $UW=0$ and $U\cap W=\{0\}$. For a submodule U of V, if the linear map of U into its dual space U° defined by $x\mapsto(x,\ )$ is an isomorphism, then we say U is nonsingular.

Now, with these notations, we state our theorem. For $\sigma\in\mathrm{Sp}(V)$ let V_σ be the fixed module of σ, i.e., $V_\sigma=\{x\in V\mid \sigma x=x\}$ and $d=\min\{\dim\overline{V_\sigma}\mid i\in I\}$. We define $l(\sigma)=0$ for $\sigma=1$.

Theorem. *For σ in $\mathrm{Sp}_n(V)$ we have the following ($^-$ denotes π_i).*

(i) *For each $i\in I$, if $\bar{\sigma}=1$ or $\bar{\sigma}^2\neq 1$, then $l(\sigma)=n-d$.*

(ii) *If $l(\sigma)\neq n-d$, then $l(\sigma)=n-d+1$.*

2. Transvections and preliminary lemma

Let $a\in\mathcal{O}$, $x,y\in V$. Assume $V=y^*\oplus\mathcal{O}x$. Then a linear map τ on V defined by $\tau=1$ on y^* and $\tau x=x+ay$ is a transvection on V if $ay\neq 0$, otherwise it is the identity map on V. τ is denoted by $\tau_{x,ay}$.

For each i in I, χ_i or $'$ denotes the canonical homomorphism of $\mathcal{O}$ into $\mathcal{O}_{A_i}$ which carries an element a of $\mathcal{O}$ to the class a' of $\mathcal{O}_{A_i}$ represented by $a/1$.

Therefore, for a and b in $\mathcal{O}$, $a'=b'$ if and only if $ca=cb$ for some c in $\mathcal{O}-A_i$. We use the same notation χ_i or $'$ to denote the canonical homomorphisms $V\to\mathcal{O}_{A_i}V$ or $\mathrm{Sp}(V)\to\mathrm{Sp}(\mathcal{O}_{A_i}V)$.

Lemma 2.1. *Let i be in I. For u and v in V, if $u'=v'$ then $cu=cv$ for some c in $\mathcal{O}-A_i$.*

Proof. Let $\{x_\lambda\}$ be a base for V. We write $u=\sum_{\lambda=1}^n a_\lambda x_\lambda$ and $v=\sum_{\lambda=1}^n b_\lambda x_\lambda$, $a_\lambda, b_\lambda\in\mathcal{O}$. Then $u'=v'$ implies $a'_\lambda=b'_\lambda$ for each λ. Hence $c_\lambda a_\lambda=c_\lambda b_\lambda$ for some c_λ in $\mathcal{O}-A_i$. Put $c=\prod c_\lambda$. $\square$

3. Proof of (i) of the theorem

For i in I, throughout this paper, $^-$ denotes π_i, $'$ denotes χ_i and ε_i denotes an element in $\mathcal{O}$ with $\pi_i\varepsilon_i = 1$ and $\pi_j\varepsilon_i = 0$ for $j \neq i$; in fact, such ε_i exists by the Chinese Remainder Theorem.

Lemma 3.1. *Let $\{E_s \mid 1 \leq s \leq r\}$ be r hyperplanes of V, then*

$$\dim \overline{\bigcap_{s=1}^{r} E_s} \geq n - r$$

for any i in I.

Proof. Take any i in I. If $r = 1$, then the lemma is clear. So let $r > 1$. Write $D = \bigcap_{s=1}^{r-1} E_s$ and $E = E_r$. We suppose $\dim \bar{D} \geq n - r + 1$ and show $\dim \overline{D \cap E} \geq n - r$, which gives us the lemma by induction on r.

To avoid the complexity of notations, we write $d = n - r + 1$. Take a base $\{\bar{x}_1, \ldots, \bar{x}_d\}$ for $\bar{D}$ where $x_1, \ldots, x_d$ are in D. Since E is a hyperplane, we have $V = E + \mathcal{O}x$, $x \in V$. Hence we may express $x_\lambda = u_\lambda + a_\lambda x$, $u_\lambda \in E$ and $a_\lambda \in \mathcal{O}$ for each $\lambda = 1, \ldots, d$.

If $a'_\lambda = 0$ for all λ, then we have an element c in $\mathcal{O} - A_i$ with $ca_\lambda = 0$ for all λ. Hence $cx_\lambda = cu_\lambda$ is contained in $D \cap E$, and so $\overline{D \cap E} = \bar{D}$. Consequently, $\dim \overline{D \cap E} > n - r$.

Next, we treat the case that at least one $a'_\lambda \neq 0$. Since $\mathcal{O}_{A_i}$ is a valuation ring, we may assume a'_1 divides any a'_λ in $\mathcal{O}_{A_i}$. Put $a'_\lambda = (b'_\lambda / c'_\lambda) a'_1$ for some b_λ in $\mathcal{O}$ and c_λ in $\mathcal{O} - A_i$. Then $(c_\lambda a_\lambda)' = c'_\lambda a'_\lambda = b'_\lambda a'_1 = (b_\lambda a_1)'$. Hence $e_\lambda c_\lambda a_\lambda = e_\lambda b_\lambda a_1$ for some e_λ in $\mathcal{O} - A_i$. Put $v_\lambda = e_\lambda c_\lambda x_\lambda - e_\lambda b_\lambda x_1$. Then v_λ is in $D \cap E$. Since c_λ, e_λ are in $\mathcal{O} - A_i$, we have $\dim \overline{D \cap E} \geq d - 1 = n - r$. □

Corollary 3.2. $l(\sigma) \geq n - d$.

Proof. Consider that transvections fix hyperplanes. Apply the lemma. □

By the corollary it suffices to show $l(\sigma) \leq n - d$. The proof will proceed by induction on $n - d$.

Lemma 3.3. *Let U be a submodule of V. If $\bar{V} = \bar{U}$ for all i in I, then $V = U$.*

Proof. Let $V = \bigoplus_{\lambda=1}^{n} \mathcal{O}x_\lambda$. Take $u_{i\lambda}$ in U with $\bar{x}_\lambda = \bar{u}_{i\lambda}$ for i in I and λ in $\{1, \ldots, n\}$. Put $u_\lambda = \sum_{i \in I} \varepsilon_i u_{i\lambda}$. Then u_λ is contained in U and $\bar{x}_\lambda = \bar{u}_\lambda$ for each i and λ. This means $x_\lambda - u_\lambda$ is in AV, where $A = \bigcap_{i \in I} A_i$. So, we may write

$$x_\lambda = u_\lambda + \sum_{\mu=1}^{n} a_{\lambda\mu} x_\mu, \quad a_{\lambda\mu} \in A.$$

Put $M = \{a_{\lambda\mu}\}$. Then we have ${}^t(u_1, \ldots, u_n) = {}^t(x_1, \ldots, x_n)(E - M)$, E is the identity matrix. Since $E - M$ is invertible, we have $V = U$. □

Let $n - d = 0$. Then by the lemma we have $V = V_\sigma$. Therefore, $\sigma = 1$ and we have $l(\sigma) = 0 = n - d$, whence there is nothing to do.

So, let $n-d>0$, i.e., $\sigma\neq 1$. We shall show that there exists τ in S such that $\min\{\dim \overline{V_{\tau\sigma}} \mid i\in I\}\geq d+1$, and, for each i in I it holds that $\overline{\tau\sigma}=1$ or $\overline{\tau\sigma}^2\neq 1$, which will imply $l(\tau\sigma)\leq n-(d+1)$ by induction on $n-d$, and so $l(\sigma)\leq n-d$ as we desire.

Definition. We define the following sets:

$$I_1=\{i\in I \mid \bar\sigma^2\neq 1\},$$

$$I_2=\{i\in I \mid \bar\sigma=1 \text{ and } \sigma'\neq 1\},$$

$$I_3=\{i\in I \mid \bar\sigma=1 \text{ and } \sigma'=1\}.$$

We have $I=I_1+I_2+I_3$ (direct sum) by assumption of (i) of the theorem.

Lemma 3.4. *Let $\mathcal{O}$ be a field and $\sigma^2\neq 1$. Then there exist x and v in V such that*
(a) $v=(\sigma-1)x$,
(b) $vx\neq 0$,
(c) *if we define $\tau=\tau_{x,v}$, then $\tau\sigma=1$ or $(\tau\sigma)^2\neq 1$.*

Proof. See Lemma 2.2 of Ishibashi [4]. □

Corollary 3.5. *Let i be in I_1. Then there exist x_i and v_i in V such that*
(a) $v_i=(\sigma-1)x_i$,
(b) $v_ix_i\notin A_i$,
(c) *if we write $\tau=\tau_{\bar x_i,\bar v_i}$, then $\tau\bar\sigma=1$ or $(\tau\bar\sigma)^2\neq 1$.*

Proof. Since $i\in I_1$, we have $\bar\sigma^2\neq 1$. Apply the lemma. □

Lemma 3.6. *Let $\mathcal{O}$ be a valuation ring with the maximal ideal A. If $\sigma\neq 1$ and $\bar\sigma=1$, then there exist x and y in V and p in $\mathcal{O}$ such that*
(a) $(\sigma-1)x=py$,
(b) $yx\notin A$,
(c) $(\sigma-1)V\subset pV$.

Proof. Let $V=\bigoplus_{\lambda=1}^{n}\mathcal{O}x_\lambda$, $x_\lambda\in V$. Since $\mathcal{O}$ is a valuation ring, we may write for each $\lambda\in\{1,\dots,n\}$

$$(\sigma-1)x_\lambda=a_\lambda y_\lambda,\quad a_\lambda\in\mathcal{O},\ y_\lambda\in V-AV$$

(in fact $a_\lambda\in A$, since $\bar\sigma=1$). Since $\sigma\neq 1$, at least one a_λ, say a_1, is not zero. Again, since $\mathcal{O}$ is a valuation ring, we may assume a_1 divides all a_λ's. Put $p=a_1$. Then by the choice of a_1 we have (c). Next, since V is nonsingular, there exists x_μ with $y_1x_\mu\notin A$. Here, to simplify the notations, we write $x_1=u$, $y_1=v$, $x_\mu=w$ and $y_\mu=z$. Further we may write $a_\mu=pe$, $e\in\mathcal{O}$. Namely, $(\sigma-1)u=pv$ and $(\sigma-1)w=pez$.

Let b, c be variables in $\mathcal{O}$, and put

$$x=bu+cw \quad\text{and}\quad y=bv+cez.$$

Then (a) holds and also the equation

$$yx = b^2vu + bc(vw + ezu) + c^2ezw.$$

Now, we shall show that we can choose b, c in $\bigcirc$ so that $yx \notin A$, i.e., we shall show (b).

First, we note that by the choice of x_μ we have

$$vw \notin A. \tag{1}$$

If $vu \notin A$ then let $b = 1$ and $c = 0$. So, from now on we assume $vu \in A$. If $e \in A$ then let $b = c = 1$. If $e \notin A$ and $zw \notin A$ then let $b = 0$ and $c = 1$. Finally, if $e \notin A$ and $zw \in A$, letting $b = c = 1$, we have

$$yx \equiv vw + ezu \mod A. \tag{2}$$

On the other hand, we have

$$\begin{aligned} 0 &= \sigma w \sigma u - wu = (w + pez)(u + pv) - wu \\ &= pwv + pezu + p^2ezv \\ &= p(wv + ezu + pezv). \end{aligned} \tag{3}$$

Suppose yx were in A. By (2) we write

$$vw + ezu = b, \quad b \in A. \tag{4}$$

Using (3) and (4), we have

$$0 = a_1(b - 2vw + aezv). \tag{5}$$

If $a_1ezv \in A$, then by (1) $b - 2vw + a_1ezv \notin A$, i.e., it is a unit. Hence $a_1 = 0$ by (5), which implies $\sigma = 1$, a contradiction. So it must be that $a_1ezv \notin A$, in particular $a_1 \notin A$. But this is impossible, because $\bar{\sigma} = 1$. Thus in each case we have a contradiction. Therefore, $yx \notin A$, this is (b). $\square$

Corollary 3.7. *Let i be in I_2. Then there exist x_i and y_i in V, a in A_i, c in $\bigcirc - A_i$ such that*

(a) $(\sigma - 1)x_i = ay_i$,
(b) $y_ix_i \notin A_i$,
(c) $(\sigma - 1)cV \subset aV$,
(d) $d < \dim \overline{V_\sigma + \bigcirc x_i}$.

Proof. Put $\varrho = \sigma'$. Then we have $\varrho \neq 1$ and $\bar{\varrho} = 1$, since $i \in I_2$. Applying the lemma to ϱ, we have p in $\bigcirc_{A_i}$, x and y in $\bigcirc_{A_i}V$ satisfying conditions analogous to (a), (b) and (c) of the lemma. Put $p = a'/b'$, $a \in \bigcirc$ and $b \in \bigcirc - A_i$. Multiplying p, x and y by a suitable element in $(\bigcirc - A_i)'$, we may assume $p = a'$ and x, y are in V'. Write $x = u'$ and $y = v'$, $u, v \in V$. Then by conditions (a) and (b), we have $(\sigma' - 1)u' = a'v'$ and $v'u' \notin A_i'$. Hence $((\sigma - 1)u)' = (av)'$ and $vu \notin A_i$. Applying Lemma 2.1, we have

$(\sigma-1)eu=aev$ for some e in $\bigcirc - A_i$. Put $x_i=eu$ and $y_i=ev$. Then we have (a) and (b) of the corollary.

Next, condition (c) of the lemma implies $(\sigma'-1)V'\subset a'\bigcirc_{A_i}V$. Since V' is finite-dimensional, this implies that $(\sigma'-1)f'V'\subset a'V'$ for some f in $\bigcirc - A_i$. Thus, applying Lemma 2.1 again, we have (c) for some c in $\bigcirc - A_i$.

Finally we show (d). Suppose $\bar{x}_i\in \overline{V_\sigma}$. Then we can write $x_i=z+u$ where $z\in V_\sigma$ and $u\in A_iV$. Since by (b) we have $y_ix_i\notin A_i$, it holds that $y_iz\notin A_i$. Put $s=y_iz$. On the other hand, we know $((\sigma-1)V)V_\sigma=0$. Hence we have $ay_iz=as=0$. Therefore (c) implies $cs(\sigma-1)V=asV=\{0\}$, which contradicts to $i\in I_2$. □

Lemma 3.8. *Let i be in I. For x and v in V, if $vx\notin A_i$, we have $\overline{v^*}=\bar{v}^*$ and $\bar{V}=\overline{v^*}\oplus\bar{\bigcirc}\bar{x}$.*

Proof. Since $\overline{v^*}\subset \bar{v}^*$ is clear, we show the converse. Take any $\bar{z}$ in $\bar{v}^*$, $z\in V$. Hence $\bar{z}\bar{v}=0$. Put $a=zv$ and $b=xv$. Then $a\in A_i$ and $b\notin A_i$. Take $c\equiv b^{-1}$ modulo A_i. Then $bcz-acx\in v^*$ and $\bar{z}=\overline{bcz-acx}$. Thus $\bar{v}^*\subset\overline{v^*}$ and so $\overline{v^*}=\bar{v}^*$.

Next, since $\bar{v}\bar{x}\neq 0$, it is obvious that $\bar{V}=\bar{v}^*\oplus\bar{\bigcirc}\bar{x}$. Hence the lemma holds. □

Lemma 3.9. *Let i be in I. Suppose $cv=aw$ for a in $\bigcirc$, c in $\bigcirc - A_i$, and v, w in V. If $wx\notin A_i$ for some x in V, then we have $\bar{V}=\overline{v^*+\bigcirc x}$.*

Proof. By Lemma 3.8 we have $\bar{V}=\overline{w^*\oplus\bigcirc x}$. Therefore it suffices to show $\overline{w^*}\subset\overline{v^*}$. Take any z in w^*. Choose s in $\bigcirc$ with $sc\equiv 1 \bmod A_i$. Then, by $sczv=sazw=0$, we have scz in v^*. Clearly $\bar{z}=\overline{scz}$. Hence $\overline{w^*}\subset\overline{v^*}$. □

Lemma 3.10. *Let i be in I_3. Then for any v in $(\sigma-1)V$ we have $\bar{V}=\overline{v^*}$. Further, there exists x_i in V with $d<\dim\overline{V_\sigma+\bigcirc x_i}$.*

Proof. Since $i\in I_3$, we have $\sigma'=1$. This means $((\sigma-1)V)'=0$. Since V is finite-dimensional, this implies $(\sigma-1)cV=0$ for some c in $\bigcirc - A_i$. Let v be any vector in $(\sigma-1)V$. So $cv=0$. Take any z in V and choose e in $\bigcirc - A_i$ with $\bar{c}\bar{e}=1$. Then $\bar{z}=\overline{cez}$ and cez is contained in v^*. Thus we have $\bar{V}=\overline{v^*}$.

The second part is clear, since we have $d<n$. □

Now, using these lemmas, we shall prove (i) of the theorem. For each i in I, we take such x_i in V as in Corollaries 3.5, 3.7 and Lemma 3.10.

We put $x=\sum_{i\in I}\varepsilon_i x_i$, $v_i=(\sigma-1)x_i$ and $v=(\sigma-1)x$. (ε_i has been defined in the beginning of this section.)

First, since $V_\sigma((\sigma-1)V)=\{0\}$, we have

$$V_\sigma\subset v^*. \tag{6}$$

Next we shall show for each i in I

$$\bar{V}=\overline{v^*+\bigcirc x} \tag{7}$$

and

$$d<\dim \overline{V_\sigma + \bigcirc x}. \tag{8}$$

If i is in I_1, then by Corollary 3.5 we have $v_i x_i \notin A_i$ and so $vx \notin A_i$. Hence by Lemma 3.8 $\bar{V} = \overline{v^*} \oplus \bar{\bigcirc}\bar{x} \supset \overline{V_\sigma} \oplus \bar{\bigcirc}\bar{x}$, which implies (7) and (8).

If i is in I_2, then by Corollary 3.7 we can write $cv = aw$ for some a in $\bigcirc$, c in $\bigcirc - A_i$, and w in V with $wx \notin A_i$. Hence by Lemma 3.9 we have (7). As for (8), it is induced by (d) of Corollary 3.7.

Finally, if i is in I_3, then Lemma 3.10 gives (7) and (8).

Thus we have proved (6), (7) and (8) for x, v. Therefore, if we apply Lemma 3.3 to (7), then we have

$$V = v^* + \bigcirc x. \tag{9}$$

Now, for each i in I, by (6) ~ (9) we can take d vectors $u_{i1}, u_{i2}, \dots, u_{id}$ in V_σ and $n-d-1$ vectors $u_{id+1}, \dots, u_{in-d-1}$ in v^* such that $\{\bar{u}_{i\lambda}, \bar{x} \mid 1 \le \lambda \le n-1\}$ is a base for $\bar{V}$. Put $u_\lambda = \sum_{i \in I} \varepsilon_i u_{i\lambda}$. Then $\{\bar{u}_\lambda, \bar{x} \mid 1 \le \lambda \le n-1\}$ is a base for $\bar{V}$, for each i in I.

Lemma 3.11. *Let $u_1, \dots, u_n$ be vectors in V. For each i in I, if $\bar{V} = \bigoplus_{\lambda=1}^n \bar{\bigcirc}\bar{u}_\lambda$, then $V = \bigoplus_{\lambda=1}^n \bigcirc u_\lambda$.*

Proof. By Lemma 3.3, we know $V = \sum_{\lambda=1}^n \bigcirc u_\lambda$. Hence we show the linear independence of $\{u_\lambda\}$ over $\bigcirc$. Suppose $a_1 u_1 + \cdots + a_n u_n = 0$, $a_\lambda \in \bigcirc$, with at least one nonzero coefficient, say a_1. We take a maximal ideal A_i which contains the annihilator of a_1. Then $a'_1 \ne 0$ in $\bigcirc_{A_i}$. Since $\bigcirc_{A_i}$ is a valuation ring, we may assume a'_1 divides all a'_λ. So we have

$$a'_1(u'_1 + (b'_2/c'_2)u'_2 + \cdots) = 0, \quad b_\lambda \in \bigcirc,\ c_\lambda \in \bigcirc - A_i.$$

Hence we have

$$a_1(e_1 u_1 + e_2 u_2 + \cdots) = 0, \quad e_\lambda \in \bigcirc,\ e_1 \in \bigcirc - A_i.$$

Since $\bar{V} = \bigoplus_{\lambda=1}^n \bar{\bigcirc}\bar{u}_\lambda$ is nonsingular, we have a vector v in V with $\overline{u_1}\bar{v} = 1$ and $\overline{u_\lambda}\bar{v} = 0$ for $\lambda \ne 1$. Put $b = (e_1 u_1 + e_2 u_2 + \cdots)v$. Then $b \in \bigcirc - A_i$ and $a_1 b = 0$, which contradicts the choice of A_i. $\square$

By the lemma, $\{u_1, \dots, u_{n-1}, x\}$ is a base for V. Put $U = \bigoplus_{\lambda=1}^{n-1} u_\lambda$. Then $V = U \oplus \bigcirc x$. Since V is nonsingular, we may choose a vector y in V with $y^* = U$, $U^* = \bigcirc y$ and $xy = 1$. Since $Uv = \{0\}$, this implies $v = ay$ for some a in $\bigcirc$.

Hence we can define $\tau = \tau_{x,-ay}$. Then $U \subset V_\tau$. Since $\bigcirc u_1 \oplus \cdots \oplus \bigcirc u_d \subset U \cap V_\sigma$, we see $\bigcirc u_1 \oplus \cdots \oplus \bigcirc u_d \subset V_{\tau\sigma}$. Moreover, by direct computation we see $\tau\sigma x = x$, i.e. $\bigcirc x \subset V_{\tau\sigma}$. Therefore, for each i in I, we have

$$\dim \overline{V_{\tau\sigma}} \ge d + 1.$$

Finally, we show we have $\overline{\tau\sigma} = 1$ or $\overline{\tau\sigma}^2 \ne 1$.

If i is in I_1, then by (c) of Corollary 3.5 we have $\overline{\tau\sigma} = \tau_{\bar{x},\bar{y}}\bar{\sigma} = \tau_{\bar{x}_i,\bar{y}_i}\bar{\sigma} = 1$ or $\overline{\tau\sigma}^2 \neq 1$.

If i is in I_2 or I_3, then we have $\bar{\sigma} = 1$. So $\bar{y}_i = 0$. Therefore $\bar{\tau} = \tau_{\bar{x}_i,\bar{y}_i} = 1$, and consequently $\overline{\tau\sigma} = 1$.

Thus, we can apply induction on $n-d$ to $\tau\sigma$ and have $l(\tau\sigma) = n-(d+1)$. Hence $l(\sigma) \leq n-d$. We have completed the proof for (i) of the theorem.

4. Proof of (ii) of the theorem

Since $l(\sigma) > n-d$, it suffices to show $l(\sigma) \leq n-d+1$. We shall reduce the case to the first by the following lemmas.

Lemma 4.1. *There exists a base* $\{x_1, \ldots, x_d, \ldots, x_n\}$ *for* V *such that* $\{x_1, \ldots, x_d\} \subset V_\sigma$, *where* $d = \min\{\dim \overline{V_\sigma} \mid i \in I\}$.

Proof. For each i in I, we take vectors $x_{i1}, \ldots, x_{id}, \ldots, x_{in}$ in V such that $x_{i1}, \ldots, x_{id}$ are contained in V_σ and $\{\bar{x}_{i1}, \ldots, \bar{x}_{in}\}$ is a base for $\bar{V}$. Put $x_\lambda = \sum_{i \in I} \varepsilon_i x_{i\lambda}$. Then by Lemma 3.11, $\{x_\lambda \mid 1 \leq \lambda \leq n\}$ is the desired one. □

Put $D = \bigoplus_{\lambda=1}^{d} \mathcal{O} x_\lambda$. Then for each i in I we have $\bar{D}^* = \overline{D^*}$, since V is nonsingular.

Lemma 4.2. *For any* $\sigma \in \mathrm{Sp}(V)$ *there exists* $\tau \in S$ *such that:*
(a) $d \leq \min\{\dim \overline{V_{\tau\sigma}} \mid i \in I\}$.
(b) *For each* $i \in I$, $\overline{\tau\sigma} = 1$ *or* $\overline{\tau\sigma}^2 \neq 1$.

Proof. Let $J = \{i \in I \mid \bar{\sigma} \neq 1 \text{ and } \bar{\sigma}^2 = 1\}$. Then for each $j \in J$ we have

$$\bar{V} = \bar{V}_{\bar{\sigma}} \perp \bar{V}_{-\bar{\sigma}} \quad \text{and} \quad \bar{V}_{-\bar{\sigma}} \neq \{0\}.$$

In particular, $\bar{V}_{-\bar{\sigma}}$ contains a nonsingular plane. We take $\bar{x}_j, \bar{y}_j \in \bar{V}_{-\bar{\sigma}}$ with $\bar{y}_j\bar{x}_j \neq 0$ for each $j \in J$. Since $D \subset V_\sigma$, we have $\bar{D} \subset \overline{V_\sigma}$. Further, since $\overline{V_\sigma} \subset \bar{V}_{\bar{\sigma}}$, we have $\bar{D} \subset \bar{V}_{\bar{\sigma}}$. Hence $(\bar{V}_{\bar{\sigma}})^* \subset \bar{D}^*$. Since $(\bar{V}_{\bar{\sigma}})^* = \bar{V}_{-\bar{\sigma}}$ and $\bar{D}^* = \overline{D^*}$, we have $\bar{V}_{-\bar{\sigma}} \subset \overline{D^*}$. This allows us to assume that y_j is contained in D^*. Choose any $v \in D^*$ and $u \in V$ with a unit vu. Further, let $b \in \mathcal{O}$ with $\pi_i(b) = 0$ for $i \in J$ and 1 for $i \in I - J$, and $a \in \mathcal{O}$ with $\pi_i(a) = 1$ for $i \in J$ and 0 for $i \in I - J$.

After taking these elements $\{x_j, y_j, u, v, b, a\}$, we define

$$x = \sum_{j \in J} \varepsilon_j x_j + bu \quad \text{and} \quad y = \sum_{j \in J} \varepsilon_j y_j + bv.$$

Then $\tau = \tau_{x,ay}$ is the desired one. Because, first, yx is a unit and so $V = y^* \oplus \mathcal{O}x$, whence τ is well defined. Second, since $\bar{a} = 0$ for $i \in I - J$, it holds that $\overline{\tau\sigma} = \bar{\sigma}$ for $i \in I - J$. Further, by a direct computation, for $j \in J$ we see $\overline{\tau\sigma}^2\bar{x} = \bar{x} + 2\bar{y}$, whence $\overline{\tau\sigma}^2 \neq 1$ for $j \in J$. Thus (b) holds.

Finally, since $y \in D^*$, (a) holds. □

Taking such τ as in Lemma 4.2, then for each $i \in I$ we have $\overline{\tau\sigma} = 1$ or $\overline{\tau\sigma}^2 \neq 1$. Hence applying (i) of the theorem we have $l(\tau\sigma) \leq n - d$ and so $l(\sigma) \leq n - d + 1$. Thus, we have completed the proof of (ii) of the theorem.

References

[1] C. Chang, The structures of symplectic groups over semilocal domains, J. Alg. 35 (1975) 457–476.

[2] J. Dieudonné, Sur les Groupes Classiques, Actual. Scient. et Ind., No. 1040 (Hermann, Paris, 1948).

[3] J. Dieudonné, Sur les generateurs des groupes classiques, Summa Brasil. Math. 3 (1955) 149–179.

[4] H. Ishibashi, Generators of a symplectic group over a local valuation domain, J. Alg. 53 (1978) 125–128.

[5] H. Ishibashi, Generators of $\mathrm{Sp}_n(V)$ over a quasi semilocal semihereditary domain, Comm. in Alg. 7 (16) (1979) 1673–1683.

[6] O.T. O'Meara, Symplectic Groups, A.M.S. Math. Surveys, Vol. 16 (Am. Math. Soc., Providence, RI, 1978).